RSA

PUBLIC SECTOR DIGITAL RISK MANAGEMENT – CHALLENGES AND OPPORTUNITIES

Dan Carayiannis
RSA Public Sector Director

BUSINESS-DRIVEN SECURITY™

ARCHER AT A GLANCE

RSA Archer Customers

1,500+ GRC deployments

48 of the Fortune 50

92 of the Fortune 100

103 Federal Govt Agencies

36 States, Cities, Counties

Customers in every marketplace:

-Government

-Banking

-Healthcare

-Insurance

-Energy

-Transportation

-Technology

-Retail…

Global Operations

~$1B revenue

2,700+ employees

1,000+ technology partners

30+ years of cybersecurity expertise

15+ years of risk expertise

Dell Technologies Subsidiary

RSA Archer Analyst Recognition

A Leader in:

- Gartner Magic Quadrant for Operational Risk Management Solutions (2017)
- Gartner Magic Quadrant for IT Risk Management Solutions (2017)
- Gartner Magic Quadrant for Business Continuity Management Planning Software, Worldwide (2017)
- Gartner Magic Quadrant for IT Vendor Risk Management (2017)
- The Forrester Wave™: Governance, Risk, And Compliance Platforms (2017)

* bankrate.com

TODAY'S PUBLIC SECTOR

- Security and Risk Management are top priorities for state CIO's
- Government organizations want to move from a reactive, restrictive approach that inhibits modernization and enhanced services to one that's resilient, adaptable and agile
- IT modernization initiatives can be costly, challenging, complex and introduce risks

TODAY'S PUBLIC SECTOR

- Ever expanding public demand for consistent and innovative government services
- New and changing leadership initiatives and priorities
- Uncertain funding streams
- Workforce transformation
  - Shortages and retention
  - Emerging workforce (millennials) driving for new levels of automation and work-life expectations

TODAY'S PUBLIC SECTOR

- Increasing public demand for information access
- Increased use of cloud based services (Legit and Shadow IT)
- IT becoming increasingly borderless - perimeter disappearing
- Accelerated adoption and expanded use of mobile, IOT and other technologies being used to support government business operations and public services

TODAY'S PUBLIC SECTOR

- Replacing legacy and outdated unsecure applications
- Consolidated and centralization initiatives
- Information silos's still exist which hinder data sharing and increase security risks
- Increased reliance on 3rd parties as an extension of daily business operations
- Cyber Insurance and Quantitative Risk Management

TODAY'S PUBLIC SECTOR

NATION STATE ACTORS

Nation-states

CRIMINALS

Petty criminals

Organized crime

NON-STATE ACTORS

Insiders

Cyber-terrorists / Hacktivists

RSA

TODAY'S PUBLIC SECTOR

- In 2017 public sector organizations became the #1 target for ransomware attacks

PRIVACY AND SECURITY

The City of Atlanta Is Still Locked Out of Files Over a Week After SamSam Ransomware Attack

An image of the city skyline at Hartsfield-Jackson Atlanta International Airport.

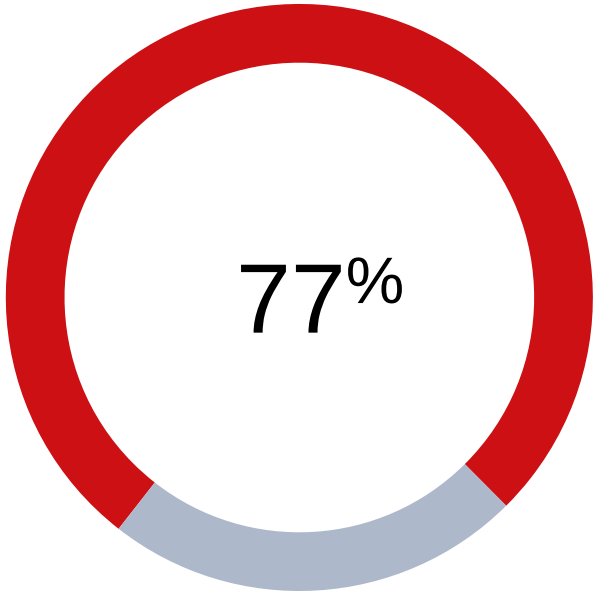
VERIZON 2017 DATA BREACH SURVEY

- Public sector organizations had the 3rd most targeted data breach victims
- 21,000+ breaches were reported among 92 public sector organizations surveyed – 239 were confirmed as DB's
- 41% contained stolen data with personal information
- More than 90% were affiliated with foreign governments

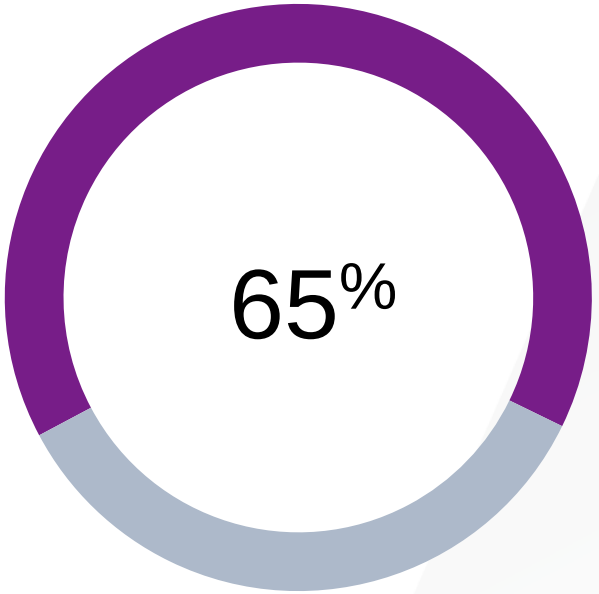
THE **RISK** CHALLENGE

RISK MANAGEMENT IS FALLING BEHIND

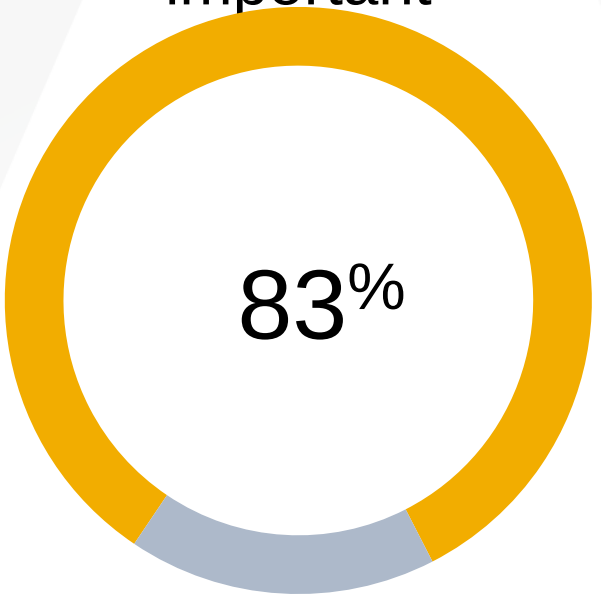
New risks
Challenge the enterprise



Risk management
is falling behind



Agility
is becoming increasingly important



From Gartner's report "The 2015 CEO and Senior Executive Survey: 'Committing to Digital', April 2015, Foundational September 2016 (Graphic created by RSA based on Figure 13. CEOs' Level of Agreement on Risk-Related Issues)

RSA

RISKS APPEAR ACROSS THE ENTERPRISE

Risks lurk underneath the surface causing cracks in your operation

Poor internal controls & governance

Litigation

Competition

Opportunities Missed

Supply Chain Interruption

3rd party non-performance, error or fraud

Human errors

Regulatory violations, fines and sanctions

Product liability claims

Employee Health & Welfare

Environmental damage

Information Security breaches

Inefficient processes & technologies

Business interruption

Unknown, unidentified risks

Internal and external fraud

RSA

MANAGING RISK IS BOTH A **BUSINESS** AND A **TECHNOLOGY** CHALLENGE

Magnitude of risk increasing

Velocity of risk increasing

Risk **Complexity** increasing

RSA

RISK GAP OF GRIEF

The **Technology** perspective…

Technology risk

- What is the important data?
- Where is the important data?
- What are the most critical applications?
- How important is this part of the infrastructure?
- What does this security event impact?
- Where are we vulnerable?
- Who are the 3rd parties the business rely on?
- What happens if IT services are disrupted?

The **Business** perspective…

Business risk

- What part of the business strategy is the most critical?
- Where are our biggest risk areas?
- What is our risk appetite and tolerance?
- What are our regulatory obligations?
- What are the most valuable pieces of our business?
- How bad could it be?
- Are we effectively managing our risks to achieve our objectives?

RSA

GAP LEAD TO RISK'S IN ONGOING OPERATIONS

Inaccurate insights & misinformation

High costs & organizational inefficiency

Unresolved findings and issues

Disconnected data & lack of context

Holes & security gaps

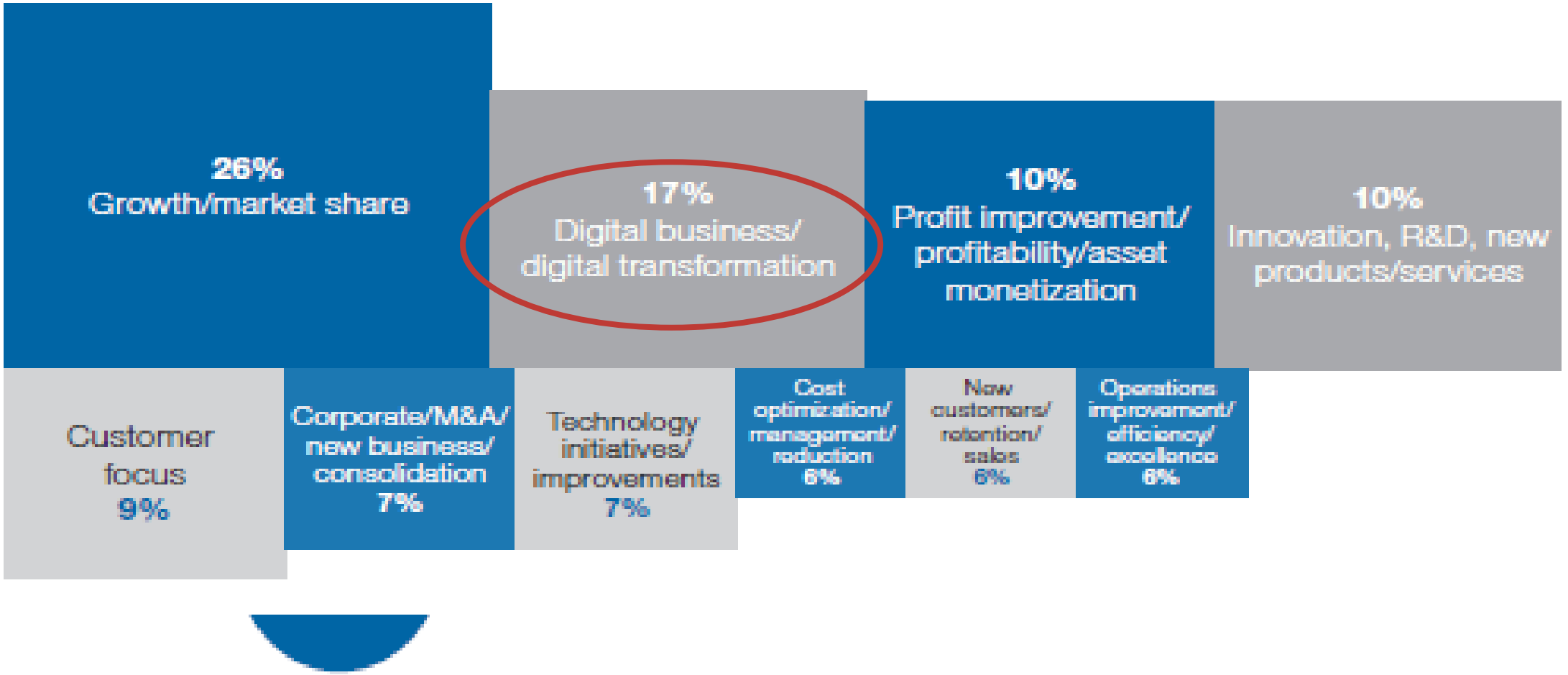
Poor business decisions & missed opportunities

RSA

DIGITAL RISK MANAGEMENT (DRM)

RSA

DIGITAL TRANSFORMATION IS UPON US…



2017 Gartner CEO Survey

RSA

DIGITAL RISK MANAGEMENT

Digital Risk *is the risk associated with transforming traditional analogue and antiquated products, processes and services to new digital platforms using digital technology*

Enablement Risks

- Implementation issues with new technology architectures, platforms, techniques, etc.
- Security & Resiliency
- Talent/skills retention
- Third party providers (tech partners, consultants, operations support)
- Data privacy, e.g. Big Data, data warehouses, etc.

Optimization Risks

- Adoption rates and organizational change management
- Interruption or downtime due to transition
- Talent/skills retention, frustration of change
- Third party providers (partners, consultants)

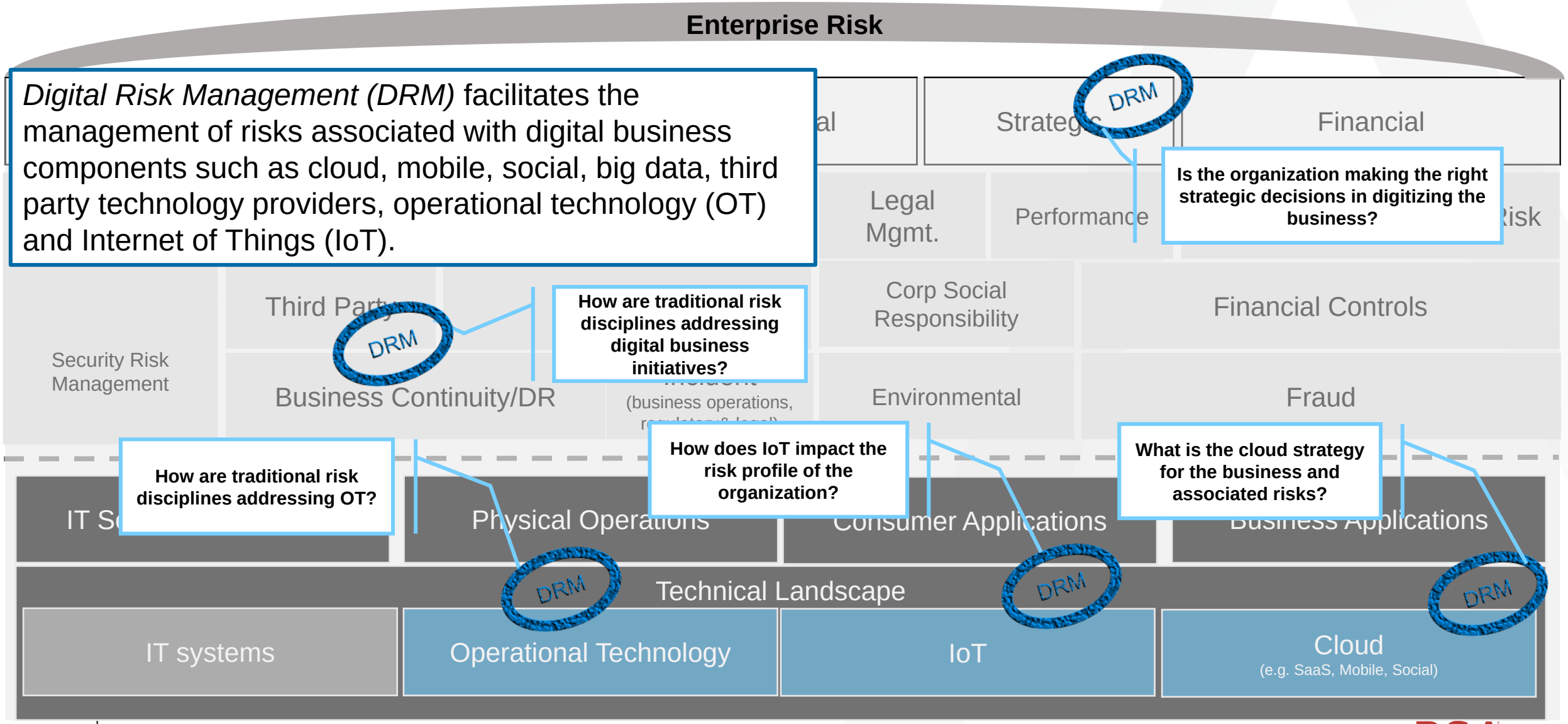
Transformation Risks

- Poor market adoption
- Opportunity costs if wrong decision is made
- High profile, reputational risks
- Financial impacts, e.g. poor ROI, cost overruns, etc.

RSA

DIGITAL RISK MANAGEMENT

Digital Risk Management (DRM) facilitates the management of risks associated with digital business components such as cloud, mobile, social, big data, third party technology providers, operational technology (OT) and Internet of Things (IoT).



DRM AND IT SECURITY

- Allows organizational leaders to see the big picture
- Better risk identification in context with prioritization
- Improves decision-making
- Better control of overall business risk
- Helps unify security practices across the enterprise
- Provides efficiency and cost savings
- Better prepares an organization for compliance with government and internal regulations

DRM AND IT SECURITY

- Allows government organizations to securely and effectively support 000’s of devices, process and applications
- Allows organizations to efficiently manage their extended IT ecosystem
- Enhanced protection and management of data that’s on premise or in the cloud
- Drives security built into everything – core servers, storage, laptops, desktops, mobile devices, physical and virtual networks
- Creates mechanisms and processes to recover data as a result of a breach or loss

DRM AND IT SECURITY

- **Back to Basics** – Update outdated policies and procedures to protect operations and data in an extended ecosystem
- **Thorough Risk Assessment** – Identify most sensitive data and understand how its protected. Understand your “crown jewel” and build an updated plan based on industry best practices to take your operations to a new more secure model
- **Continuous Risk Assessments** – Implement continuous data monitoring and frequent (weekly) risk management reviews of critical operations and conduct “what if” scenarios to test cybersecurity and incident response plans

RSA

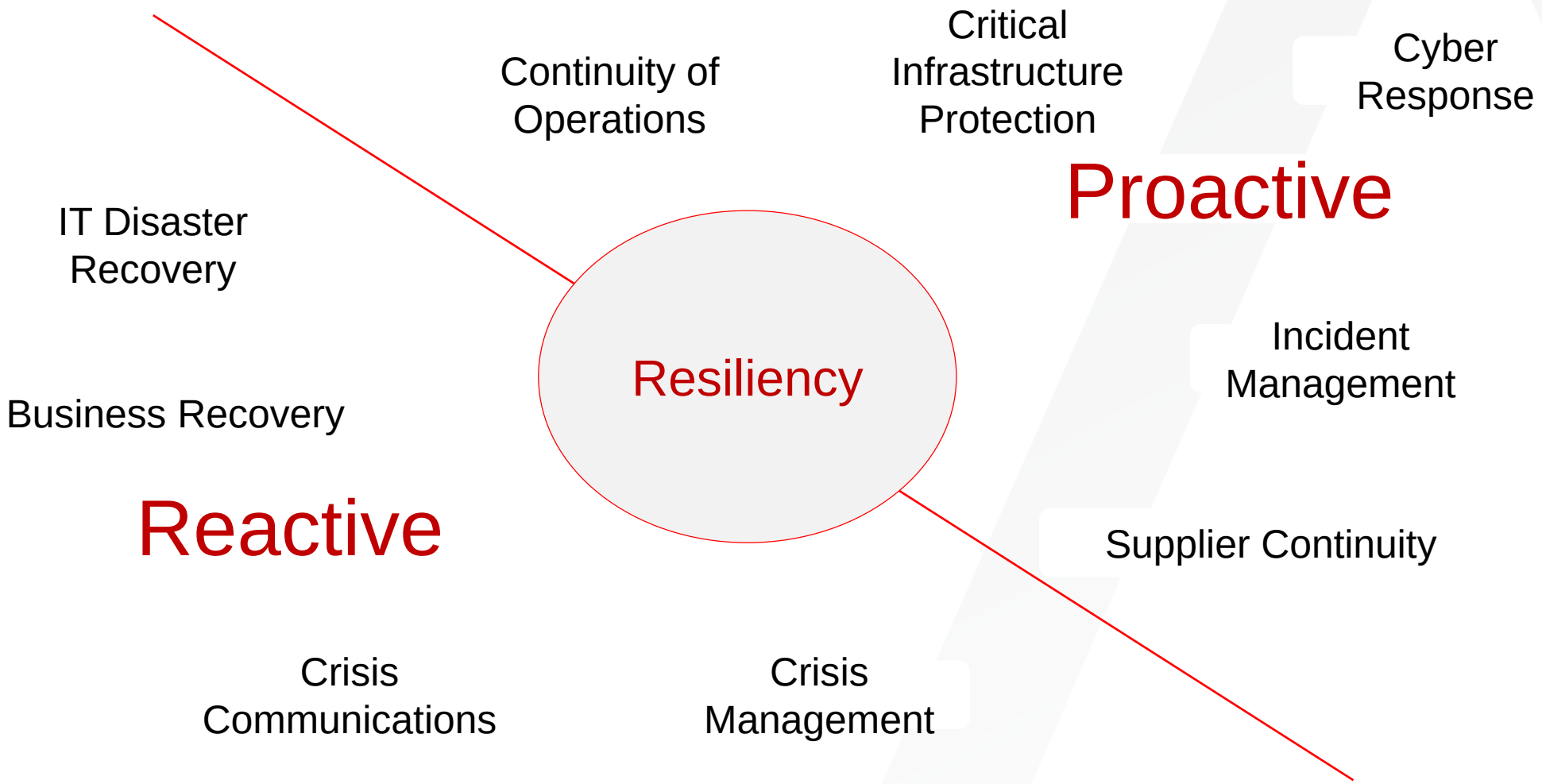
DRM AND IT SECURITY

- **Centralize Governance** – Centralized cybersecurity governance and operations becoming increasingly important to accurately understand risk and ensure consistent application of security controls
- **Build a culture of awareness** – End-user security awareness training including leadership key to mitigating and minimizing risks – people, process and technology
- **Metrics, Scorecards and Dashboards** – You need to know where you are and how your doing against baselines. Identify goals, metrics and leading indicators to measure effectiveness and track progress over time

DRM AND IT SECURITY

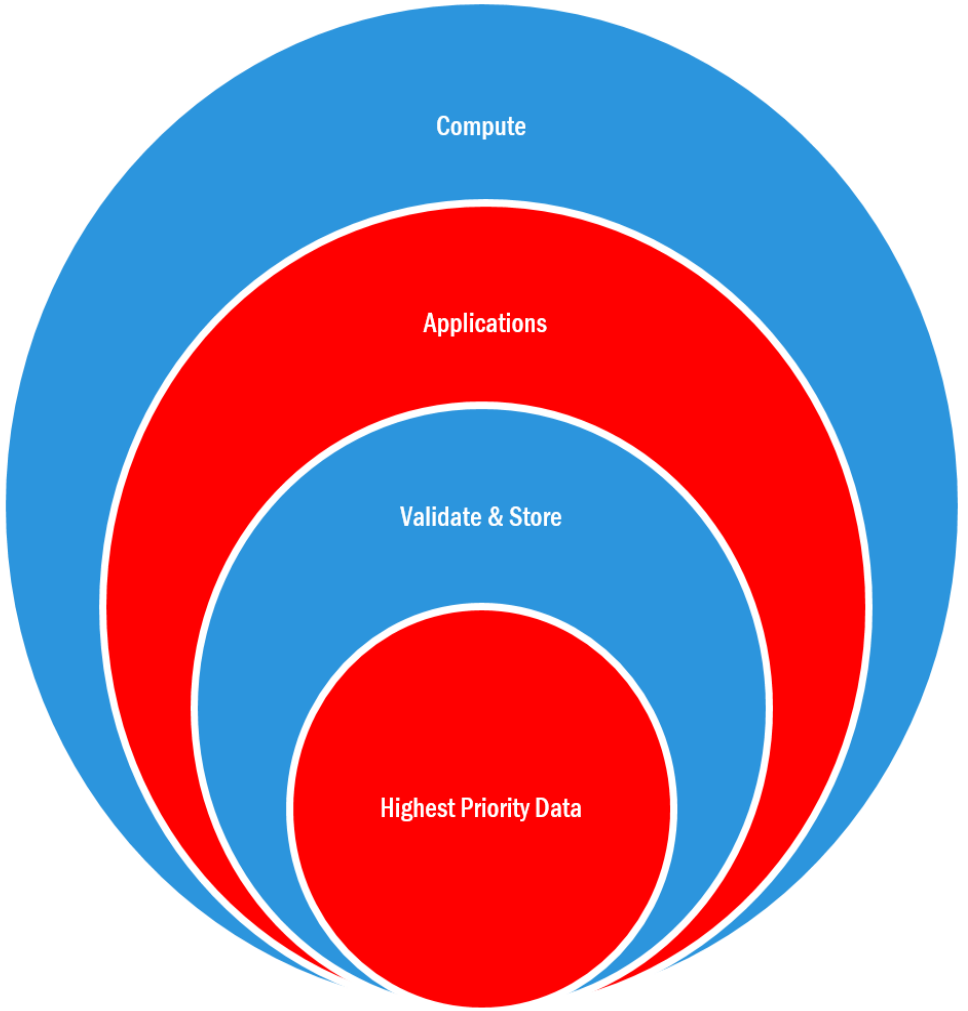
- **Understand your extended ecosystem** – Fully understand your key vendors cybersecurity maturity and validate often
- **Build in Resiliency** – Be prepared for the inevitable, create and update contingency plans, training employees and have system and data backups in place to minimize impact

RESILIENCY = PROACTIVE + REACTIVE CAPABILITIES



PROACTIVE RESILIENCY

- Helps define and protect what's most critical to the organization
- Reduces the risk of IT and business operations
- Minimizes disruptions, harmful events and significant organizational crises
- Establishes a common taxonomy and structure to identify, measure and monitor risks and events
- Respond, adapt and ensure operational continuity
- Lower overall organizational risk and reduce compliance related activities
- Drives 3rd party readiness
- Reduce costs related to disruptive events



RSA

FINAL THOUGHTS

- Government organizations face increasing demands as well as public serving opportunities
- Understanding and managing digital risk is key to public sector modernization initiatives
- Create and execute and integrated risk management vision
- Public demand for enhanced, secure and continual services is constant and growing – so are cyber threats
- Digital risk management coupled with ongoing IT security best practices provides the organizational agilely necessary to meet growing public demands as well as operational objectives

RSA

THANK YOU

Dan Carayiannis

dan.carayiannis@rsa.com